IMPLEMENTAÇÃO DO ALGORITMO SHA-256 EM CIRCUITO INTEGRADO DE APLICAÇÃO ESPECÍFICA

Lucas Daudt Franck

Prof. Dr. Maximiliam Luppe

Escola de Engenharia de São Carlos / Universidade de São Paulo

ldfranck@usp.br

Objetivos

O algoritmo SHA-256 é uma função de hash criptográfico amplamente usada na validação da autenticidade, integridade e identidade de informações digitais. Apesar de muito utilizada, a função SHA-256 tem um elevado custo computacional para ser calculada, o que motiva a busca por alternativas de aceleração por hardware, especialmente circuitos integrados de aplicação específica (ASICs). Assim, o trabalho teve como objetivos conhecer o fluxo de projeto de circuitos integrados digitais, estudar o funcionamento do algoritmo de hash criptográfico SHA-256, e projetar um circuito integrado na tecnologia de 130nm da SkyWater para computar a função de hash SHA-256.

Métodos e Procedimentos

A forma canônica do algoritmo criptográfico SHA-256 disponível na publicação FIPS180-4 *Secure Hash Standard* (2002) do NIST [1] foi descrita em Verilog e sintetizada na tecnologia alvo SKY130 através da ferramenta de código aberto OpenLANE [2]. O OpenLANE é uma rotina automatizada de projeto de circuitos integrados digitais capaz de transformar uma descrição RTL nos arquivos geométricos GDSII necessários para a fabricação do componente. O fluxo de projeto do circuito integrado adotado está ilustrado na Figura 1, com a ferramenta OpenLANE sendo responsável pelas partes de síntese, *layout* e verificações (*signoff*).

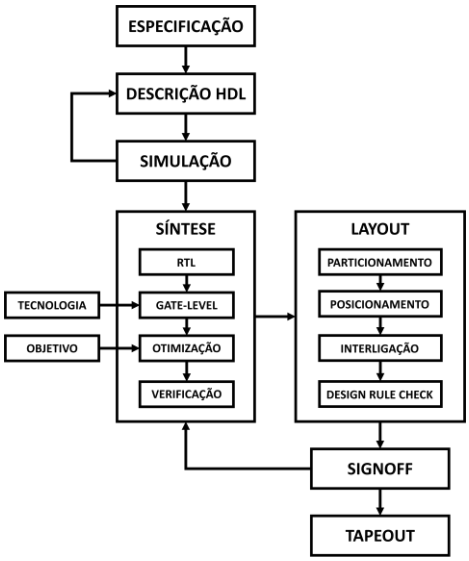

Figura 1: Fluxo de projeto de circuitos digitais.

O funcionamento do algoritmo SHA-256 é dividido em dois módulos: Bloco de Expansão, e Bloco de Compressão [3]. A dinâmica desses blocos está explicada detalhadamente em [1]. Os diagramas lógicos das estruturas descritas em Verilog para esses dois módulos estão ilustradas na Figura 2.

Na etapa de síntese, a descrição em Verilog foi carregada no OpenLANE juntamente com o *process design kit* (PDK) da tecnologia SKY130 de 130nm da SkyWater, e as configurações de da ferramenta. Uma análise exploratória dos parâmetros foi realizada para maximizar a velocidade e diminuir a área do circuito gerado.

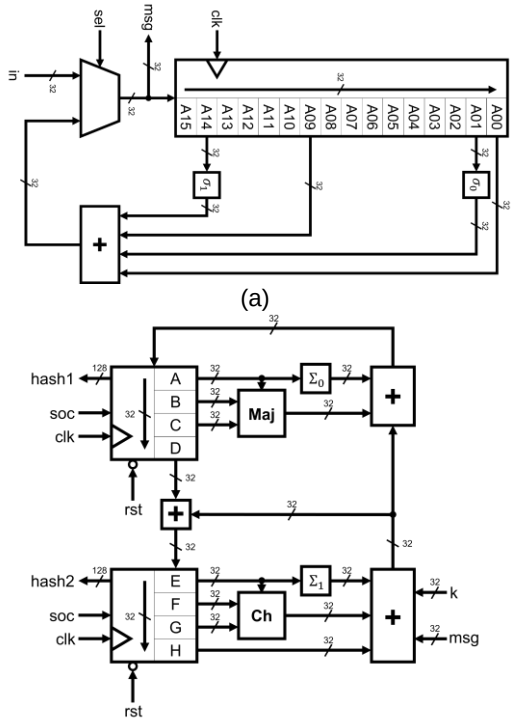

Figura 2: Blocos de (a)Expansão e (b)Compressão.

A Figura 3 ilustra o gráfico de resultados de uma das análises exploratórias feitas. Nesse estudo foram variadas a topologia de somador empregada e a estratégia de síntese, além do período alvo do sinal de *clock.* Com os resultados obtidos foi possível fazer uma busca local das configurações que apresentaram melhor área e frequência máxima de operação.

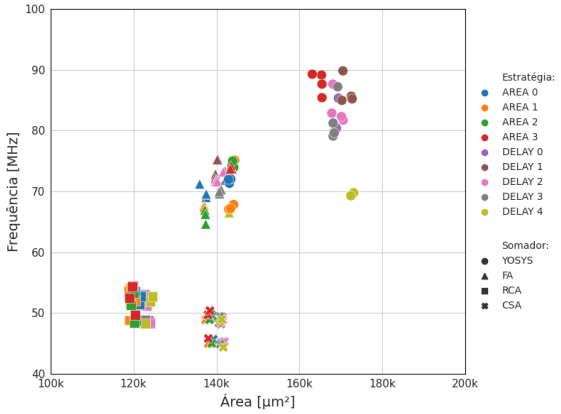

Figura 3: Resultados análise exploratória.

Resultados

A versão final do circuito integrado apresentou frequência máxima de 100,38MHz, área do núcleo de 123753µm², e utiliza de 65 ciclos de *clock* para computar um bloco do SHA-256. Os parâmetros de síntese utilizados foram: somador YOSYS, estratégia AREA 3, período de *clock* 11ns, e densidade do núcleo de 66%. Na Figura 4 está *layout* final do componente.

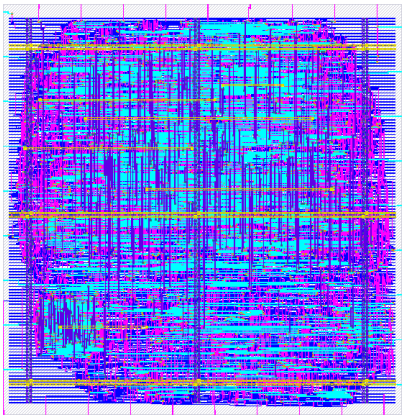

Figura 4: *Layout* do circuito integrado.

Conclusões

O circuito integrado projetado apresentou desempenho mediano quando comparado com outras implementações (por exemplo [3]). O *layout* final tem área do núcleo menor que circuitos que utilizam técnicas de *pipelining* e reestruturação do caminho crítico, mas frequência máxima de operação inferior a essas outras abordagens de projeto. Futuras otimizações de descrição podem ser realizadas para melhorar o desempenho do circuito.

Referências

[1] NIST. Secure Hash Standard (SHS). Federal Information Processing Standards Publication. FIPS180-4, ago. 2015 (revisão).
[2] SHALAN, M.; EDWARDS, T. Building OpenLANE. IEEE/ACM ICCAD. NY, USA 2020.
[3] DADDA, L.; MACCHETTI, M.; OWEN, J. The design of a high speed ASIC unit for the hash function SHA-256. IEEE. Paris, FR 2004.